UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

27510 7590 03/02/2006

KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER	
JARRETT, SCOTT L	

ART UNIT	PAPER NUMBER
3623	

DATE MAILED: 03/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/805,279	BARNHART, ROBERT M.	
	Examiner	Art Unit	
	Scott L. Jarrett	3623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This non-final office action is in response to applicant Request for Continued Examination filed December 22, 2005. Applicants amendments amended the Specification, Abstract, Drawings, canceled Claims 1-28 and added new Claims 29-33.

Response to Amendment

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.

Response to Arguments

3. Applicant's arguments with respect to claim 29-33 have been considered but are moot in view of the new ground(s) of rejection.

It is noted that the applicant did not effectively challenge the Official Notice(s) cited in the previous office actions therefore those statements as presented are herein after prior art. Specifically it has been established that it was old and well known in the art at the time of the invention:

- to represent a document as an image (e.g. graphical ballot);

- to use one-way hash functions for data integrity in conjunction with digital signature schemes;

- that cryptographic hash functions generate a hash-value which serves as a compact representative image (imprint, digital fingerprint, message digest) of an input string that can be used to uniquely identify the hashed message/string;

- that X.509 is a known digital certificate standard; and

- that signing a message provides a mechanism for determining the authenticity and integrity of a message.

Title

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Method for Verifying a Ballot Using Public Key Encryption and Digital Signatures.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 29, 30 and 33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding Claims 29 and 33, Claims 29 and 33 recite $DS(B_{cast}, s)$, lower case s, and $DS(B_{cast}, \mathbf{S})$, upper case S, where s (S) is best understood to be the private key of the server (system). Examiner requests clarification of the differences/intended distinction between the system's private key represented as a lower case s and upper case S and suggests Applicant's amend the claims to positively recite the intended differences/distinctions. Appropriate correction is required.

For the purposes of examination the examiner interpreted Claim 29 to read "comparing $DS_{\text{received token}}(B_{cast}, s)$ and ~~at least one of~~ $DS(B_{cast},s)$ ~~and $DS(B_{cast},S)$~~."

For the purposes of examination the examiner interpreted Claim 33 to read "comparing $DS(B_{cast}, s)$ and $DS(B_{cast},s)$ ~~$DS(B_{cast},S)$~~" .

Regarding Claim 30, Claim 30 recites the limitation "a digital signature of **the aggregation**" in Claim 29. There is insufficient antecedent basis for this limitation in the claim.

Examiner interpreted Claim 30 to read "a digital signature of **a** ~~the~~ aggregation" for the purposes of examination.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 29-30 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 29 and 33 Shrader et al. teach a method and system for verifying a (cast) ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8):

- forming (generating, creating, signing, encrypting, etc.) a digital signature of a (cast) ballot using the private key of a system (server; "The voting tabulator signs, encrypts and sends the encrypted electronic ballot to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and singed with the validator's private key; Paragraph 0063; Figures 7-8, Element 72);

- associating (storing, linking, relating, etc.) the (cast) ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71);

- forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- making the message available to a user (entity, voter, system, subsystem, third party, etc.; e.g. verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- receiving the message (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8, Elements 72-74);

- extracting (decrypting, stripping, de-signing, deciphering, etc.) the ballot number and the system's digital signature from the message (verification message(s) exchanged between tabulator to mediator; Paragraph 0063; Figures 7-8, Elements 73-75);

- for ballot number equal to the ballot number extracted from the message comparing the system's digital signature of the ballot extracted from the message and system digital signature of the ballot (i.e. comparing the received system digital signature to a known/calculated/accepted/certified of the system; Paragraph 0063; Figures 72-75); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that (cast) ballot (message, token, etc.) is verified (valid, authentic, genuine, unaltered, secure, etc.; Paragraphs 0061, 0063; Figures 72-75).

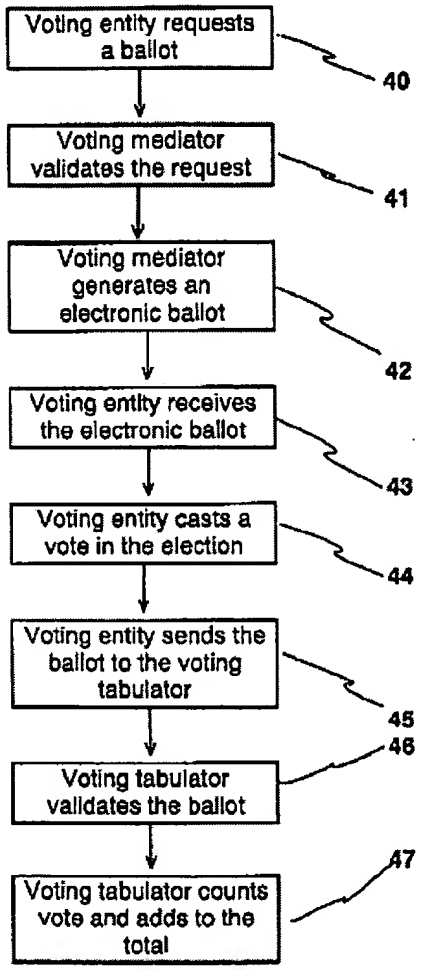

FIG. 4

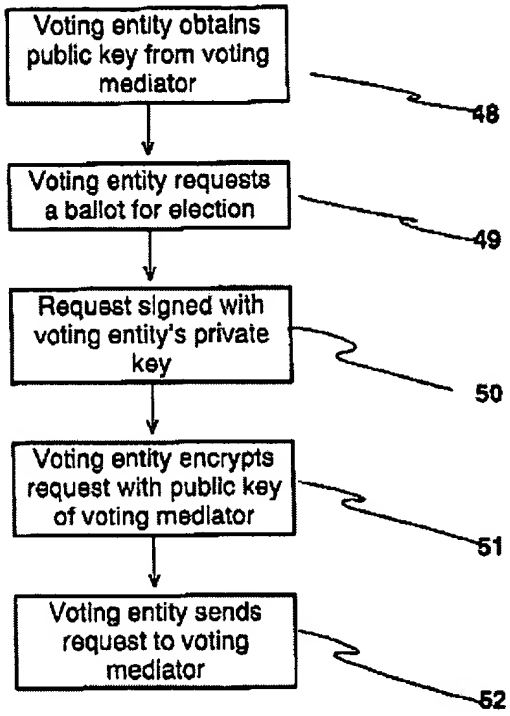

FIG. 5

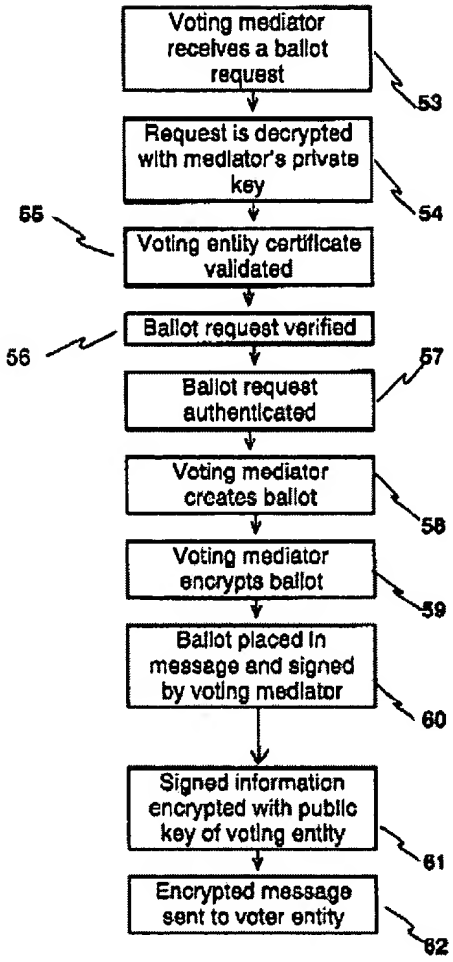
Voting mediator receives a ballot request
53
Request is decrypted with mediator's private key
54
55
Voting entity certificate validated
Ballot request verified
56
57
Ballot request authenticated
Voting mediator creates ballot
58
Voting mediator encrypts ballot
59
Ballot placed in message and signed by voting mediator
60
Signed information encrypted with public key of voting entity
61
Encrypted message sent to voter entity
62

FIG. 6

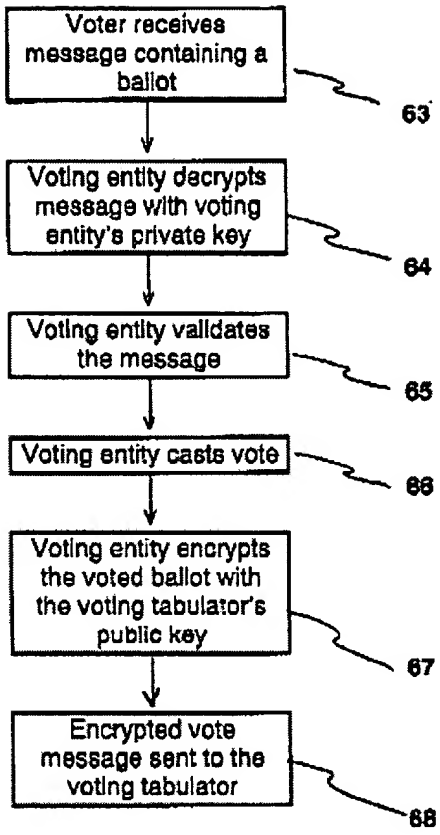
Voter receives message containing a ballot
63
Voting entity decrypts message with voting entity's private key
64
Voting entity validates the message
65
Voting entity casts vote
66
Voting entity encrypts the voted ballot with the voting tabulator's public key
67
Encrypted vote message sent to the voting tabulator
68

FIG. 7

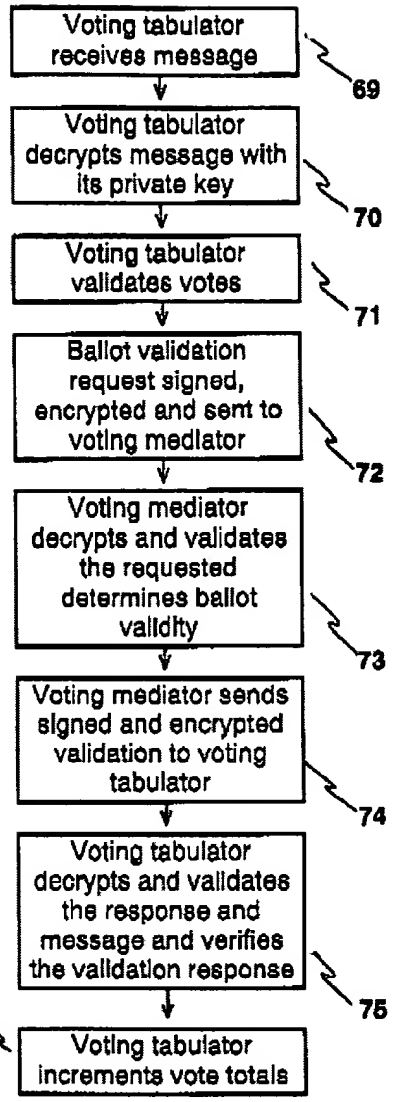

FIG. 8

Regarding Claim 30 Shrader et al. teach a method and system for verifying a ballot recorded in a system wherein the message (confirmation token, received token) further comprises the system's digital signature of the ballot and ballot number (aggregation; Paragraphs 0060-0062); and wherein the method further comprises the steps of:

- extracting a digital signature of the ballot and ballot number (aggregation) from the message (received token; Paragraphs 0060, 0061, 0063; Figures 6-8); and

- verifying (validating, accepting, certifying, authenticating, confirming, etc.) the (cast) ballot only when the digital signature of the ballot and ballot number (aggregation) extracted from the received message/token is equivalent (matches, equals, etc.) to digital signature digital signature of the ballot and ballot number (aggregation; i.e. comparing the received system digital signature to a known/calculated/accepted/certified system digital signature; Paragraphs 0061, 0063; Figures 6-8; Elements 67-75).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System (1996) in view of Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 31 Cranor et al. teach a method and system for verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising (Abstract; Figures 1,3):

- receiving, in a system (server, computer, terminal, device, etc.), at least one set of a (cast) ballot and a voter's digital signature of the ballot (Paragraph 2, Page 5);

- forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5);

- associating (storing, linking, relating, etc.) the (cast) ballot, voter's digital signature of the ballot and the voter's identification number (Paragraphs 3-4, Page 7);

- forming a message (confirmation token, string, receipt, acknowledgement, etc.) comprising system's digital signature of the cast ballot, the voter's digital signature of the cast ballot, and the system's digital signature of the aggregation of the cast ballot,

the voter's digital signature of the ballot and the system's digital signature of the ballot ("validator", "tallier", "validation certificate", "receipt"; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- making the message (token, string, etc.) available to a user (entity, voter, system, subsystem, third party, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- receiving the messages (confirmation, token, verification, acknowledgement, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- extracting (decrypting, stripping, etc.) *at least one of the following* from the message Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot;

  - system's digital signature of the ballot; ***or***

  - system's digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation);

- for extracted ballot number and the corresponding ballot number comparing *at least one of the following* (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot extracted from the message and voter's digital signature of the ballot;
  - system's digital signature of the ballot extracted from the message and system's digital signature of the ballot, **or**

- system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation) extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that the (cast) ballot is verified (valid, authentic, genuine, unaltered, accepted, counted, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

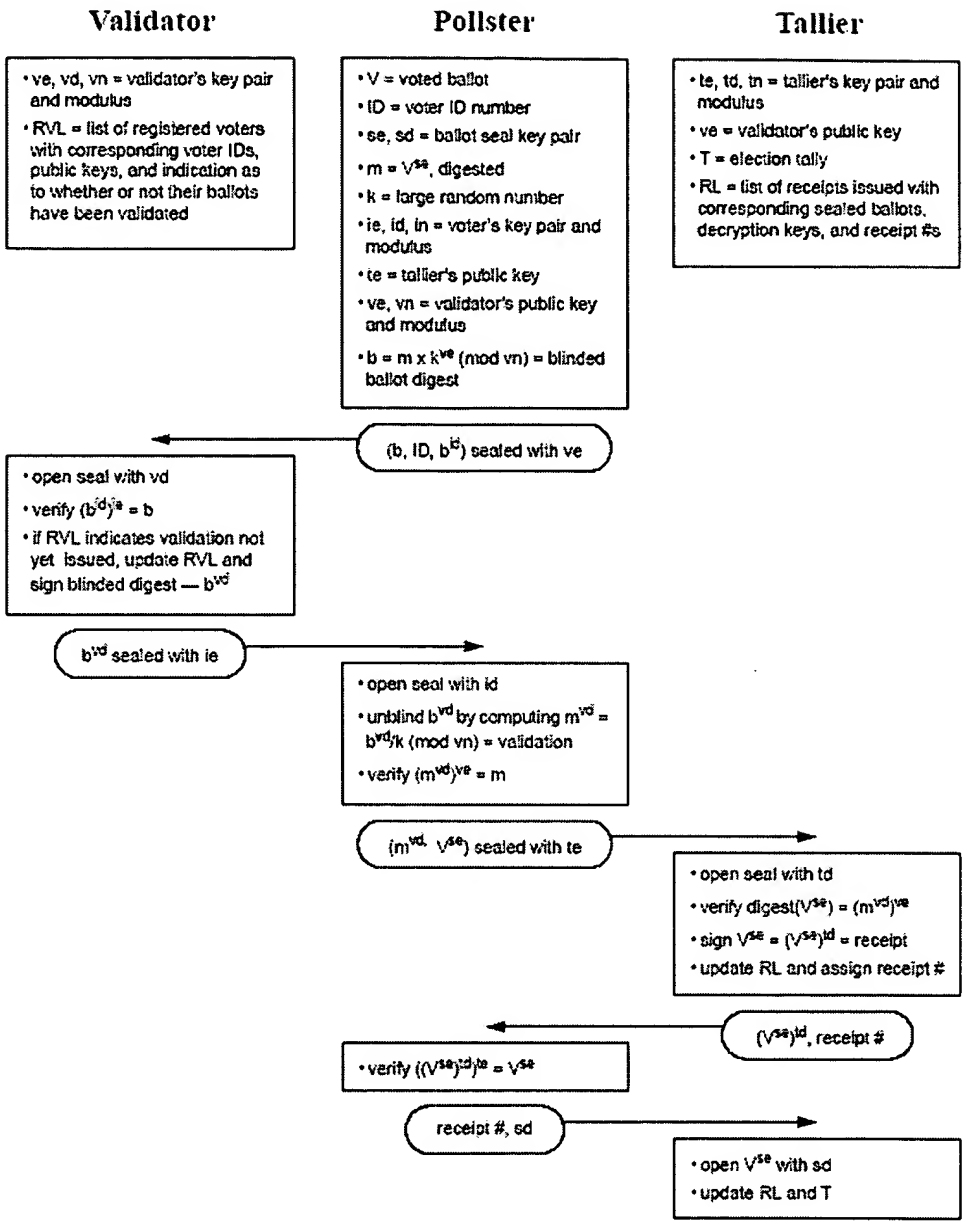

Figure 1: Blind Signature Protocol Overview

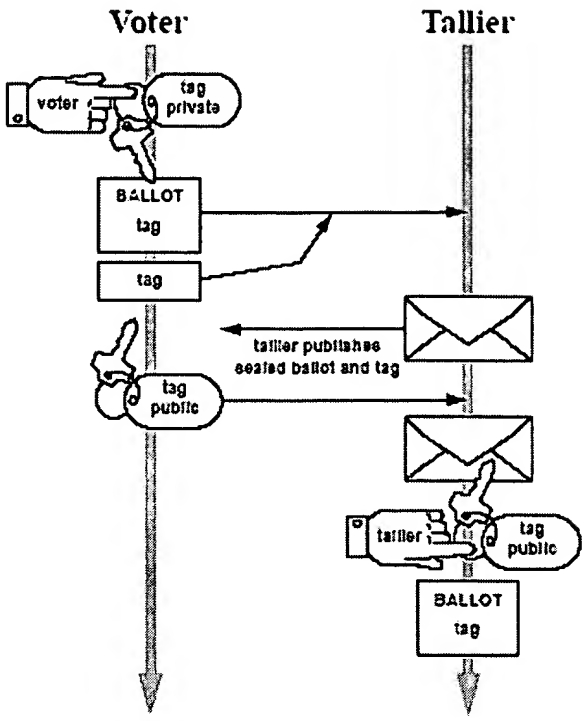

Figure 3: Phase 2 of the Two Agency Protocol

While the use of unique identifiers for (paper and/or electronic) ballots is a common business practice Cranor et al. does not expressly teach that the cast ballot includes a vote serial number as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting over a network for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only vote once (Shrader et al.: Paragraph 0063).

Regarding Claim 32 Cranor et al. teach a method and system for verifying a cast ballot recorded in a system further comprising if the comparison shows equivalence between the system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot and the system's digital signature of the ballot (aggregation) determining that the message (token) has not been modified (altered, disturbed, edited, etc.) since its formation (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8).

Cranor et al. does not expressly teach that ballots further comprise vote serial numbers as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting for the purposes of ensuring

voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only cast their ballot once (Shrader et al.: Paragraph 0063).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Fischer, Jean-Bernard, U.S. Patent No. 6,021,200, teaches a system and method for verifying a cast ballot stored on a server comprising vote serial number (ballot id), public/private key encryption, digital signatures (including but not limited to digital signature of the cast ballot/vote), confirmation tokens/messages and comparing received tokens (values, message, strings) to known/expected tokens in order to determine if a message (ballot, vote, signature, etc.) is valid (authentic, valid, genuine, etc.).

- Sussman, Lester, U.S. Patent No. 6,836,765, teaches a system and method for verifying, securing, encrypting and signing messages (commercial transactions) utilizing well known and established security protocols, standards and approaches (e.g. digital certificates, PGP, public/private key encryption, SSL, etc.).

- Gibbs, Sr. Athan, U.S. Patent No. 6,865,543, teaches a system and method for verifying a cast ballot stored on a server/system comprising forming a digital signature of the cast ballot, forming a validation receipt comprising a voter validation number and validating the authenticity of the cast ballot and validation receipt using well known cryptographic techniques, standards and technologies.

- Babbit et al., U.S. Patent No. 6,873,966, teaches a system and method for verifying a cast ballot (vote) stored in the system (on a server) wherein the system/method forms "sealed ballots" (encrypted and signed, $DS(B_{cast})$, $E(B_{cast})$,

DS(Agg)), voter specific/unique ballots and confirmation/receipts as well as utilizes digital certificates, public/private key encryption, smart cards, SSL and hash functions.

- Neff, Andrew, U.S. Patent No. 2002/0128978, teaches a system and method for verifying a cast ballot stored in a system (on a server) comprising forming digital signatures of the cast ballot, voter identification, validity proofs and other information (DS(Agg)) as well as providing users with confirmation tokens/messages based on the comparison of received and known/expected vote/ballot, system and voter data.

- Karro et al., U.S. Patent Publication No. 2002/0077885, teaches a system and method for managing electronic voting/balloting using a plurality of well-known cryptographic techniques, standards and technologies. Karro et al. further teach that the system and method forms digital signatures of cast ballots, which include at least a vote serial numbers (ballot ID) and voter IDs using the private key of the server/system.

- Best et al., U.S. Patent Publication No. 2002/0083126, teaches a system and method for managing elections (voting, balloting) over the Internet.

- Nippon Telegraph & Telephone, JP 10074046A (1998), teaches a system and method for electronic voting wherein the system/method forms digital signatures of aggregate vote/ballot data for the purposes of authenticating the cast ballot/vote.

- Cohen et al., A Robust and Verifiable Cryptographically Secure Election Scheme (1985) teaches a system and method for holding a secure ballot election using well known cryptographic techniques and tools.

- Iverson, Kenneth, A Cryptographic Scheme for Computerized General Elections (1991) teaches a system and method for performing secure electronic voting

over a network using well known cryptographic standards for verifying cast ballots including but not limited to homomorphism, tokens (vote serial number, un-reusable eligibility tokens), digital signatures, public/private encryption and the like.

- Nurmi et al., Secret Ballot Elections in Computer Networks (1991), teaches a system and method for holding electronic elections wherein voters can verify and recast cast ballots stored in the system (on a server) using the well known protocol for the "selling of secrets" known as all-or-nothing disclosure of secrets (ANDOS) approach.

- Jan, Jinn-Ke et al., teach a system and method for conducting electronic voting using well known security protocols, techniques and approaches. Jan et al. further teach that the secure anonymous voting system and method forms a message/token comprising the system's digital signature, cast ballot, and a unique ballot ID.

- Radwin, Michael, An untraceable, universally verifiable voting scheme (1995) teaches a secure electronic voting/balloting system and method using well known cryptographic techniques, standards and tools.

- Cramer et al., Multi-authority secret-ballot elections with linear work (1995) teach a system and method for verifying cast ballots using well known verifiable secret sharing techniques/approaches "proofs of validity") such that users (voters, third parties, etc.) can verify that a voter cast a legitimate ballot without divulging the exact nature of the vote/ballot (universally verifiability).

- Cranor, Lorrie Faith, Electronic Voting (1996) teaches a plurality of desired characteristics of electronic voting/balloting systems/methods including but not limited to verifiability (e.g. individual verifiability) and privacy. Cranor further teaches the use of a

plurality of well known cryptographic protocols to achieve the desired electronic voting/balloting characteristics including the use of public/private keys, voter identification numbers and "secret identification numbers" wherein the secret identification numbers are distributed to each voter prior to the election and used to ensure valid voters only cast one ballot (i.e. vote serial number).

- Baker, Dixie et al., PCASSO: Applying and Extending State-of-the-Art Security in the Healthcare Domain (1997) teaches a system and method for securing sensitive messages between a plurality of entities (systems, users, doctors, patients, insurers, etc.) over a network wherein the system/method utilizes a plurality well known and widely practiced security and cryptographic techniques, tools and technologies.

- Mu, Yi et al., Anonymous Secure E-Voting over a Network (1998) teaches a system and method for secure electronic voting/balloting over a network. Mu et al. further teach that electronic voting systems can be classified into two types non-anonymous and anonymous wherein non-anonymous systems/methods "must strictly hide the votes in order to preserve the privacy of votes" (e.g. secret sharing schemes, zero knowledge proofs) and anonymous systems hide the identify of voters but leave the contents of the votes open/unhidden.

- Baker, Dixie et al., Assurance: the power behind PCASSO security (1999) teaches a system and method for conducting "assured" communications over public networks such as the Internet wherein the system/method utilizes a plurality of well known and widely used security and cryptographic techniques (smart cards, public key infrastructure, X.509, SSL, etc.).

- Schoenmakers, Berry, Fully Auditable Electronic Secret-Ballot Elections (2000) teaches an electronic voting/balloting system and method wherein voters submit signed and encrypted ballots to the system (bulletin board) as well as proofs of validity of the vote using zero-knowledge proof techniques.

- Adler, James et al., Computational Details of VoteHere Homomorphic Election System (2000) teaches an electronic voting/balloting system and method that provides for the universal verification/validation of cast ballots wherein encrypted and signed ballots as well as proofs of a ballots validity are formed and verified/validated using well known and widely used cryptographic techniques and technologies.

- Gerck, Eric, Overview of Certification Systems (2000) teaches the use of a plurality of well known digital certificate (digital signatures) technologies/techniques including but not limited to X.509 wherein "certificates introduce tamperproof attributes which can be used as convenient references for someone receiving a message decide whether that message, the key and possibly the sender's name are what they appear to be – without asking the sender."

- VoteHere.net Web Pages (2000) teaches a commercially available system and method for conducting electronic voting/balloting over the Internet. The VoteHere.net web pages further provide explanation of well known cryptographic tools and techniques (digital signatures, hash functions, certificate authorities, public/private keys, etc.) and their application to electronic voting/balloting including but not limited to the use of ballot IDs (vote serial numbers) in individually verifiable elections for such things are countering bit commitment attacks on the confirmation message (receipt) wherein the

message comprises the ballot serial number, ballot and other information that is digitally signed by the server and provided to the voter.

- Schneier, Bruce, Applied Cryptography (1996) teaches a plurality of old and very well known cryptographic tools, techniques, methods and technologies.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott L. Jarrett whose telephone number is (571) 272-7033. The examiner can normally be reached on Monday-Friday, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (571) 272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SJ
2/22/2006

Susanna Diaz
SUSANNA M. DIAZ
PRIMARY EXAMINER
AU 3623